Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciência
Instituto de Matemática e Estatística

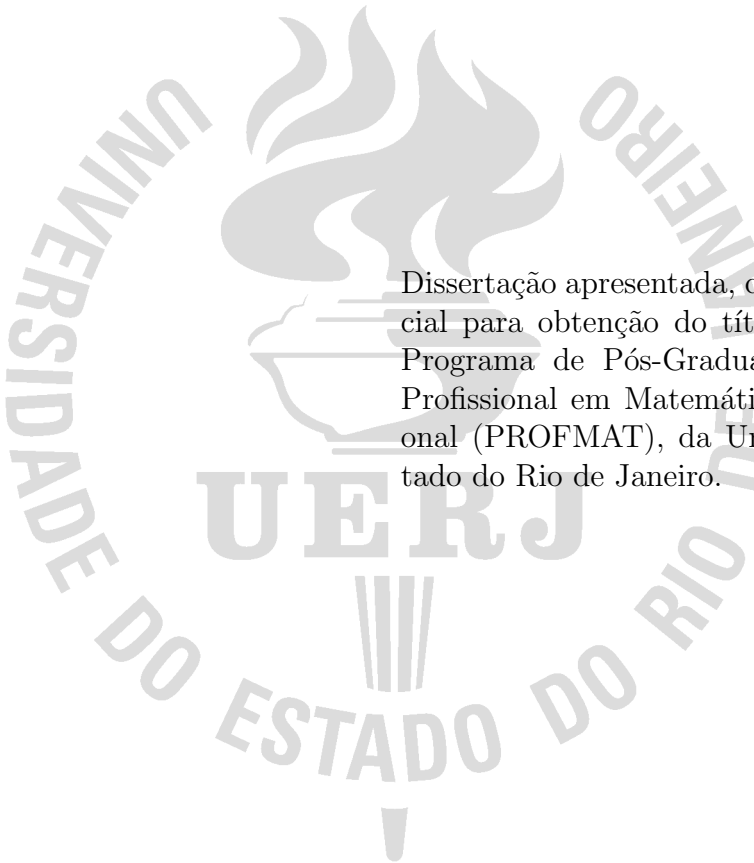
Clarissa Duarte Loureiro de Melo

Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes

Rio de Janeiro
2014

Clarissa Duarte Loureiro de Melo

Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes



Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Orientador: Prof. Dr. Roberto Alfonso Olivares Jara

Rio de Janeiro

2014

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC/A

M528 Melo, Clarissa Duarte Loureiro de
Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes / Clarissa Duarte Loureiro de Melo. – Rio de Janeiro, 2014-
53 f. : il.

Orientador: Roberto Alfonso Olivares Jara
Dissertação (Mestrado Profissional em Matemática em Rede Nacional / PROFMAT) – Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística
, Programa de Pós-Graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), 2014.

1. Matrizes (Matemática) - Estudo e ensino.. 2. Criptografia.. 3. Matemática (Ensino Médio).. I. Jara, Roberto Alfonso Olivares. II. Universidade do Estado do Rio de Janeiro.Instituto de Matemática e Estatística . III. Título

CDU: 512.643:37

Assinatura

Data

Clarissa Duarte Loureiro de Melo

Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Aprovada em 18 de Dezembro de 2014.
Banca Examinadora:

Prof. Dr. Roberto Alfonso Olivares Jara
Instituto de Matemática e Estatística - UERJ

Prof. Dr. Sérgio Luiz Silva
Instituto de Matemática e Estatística - UERJ

Prof. Dra. Cristiane de Mello
Escola de Matemática
Centro de Ciências Exatas e Tecnologia - UNIRIO

Rio de Janeiro
2014

AGRADECIMENTOS

Ao meu marido, Luciano Melo, por trilhar comigo esse caminho, me estendendo a mão sempre que precisei. Sem ele, eu não teria conseguido!

Ao meu filho, Felipe, pela sua imensa paciência e generosidade em lidar com minhas ausências.

À minha mãe, pelos constantes suporte e incentivo.

À minha ilustre companheira de trabalho, Isabel, pelo seu incansável apoio.

Aos amigos, Ivana e Adriano, pelo suporte técnico prestado ainda que à distância.

Aos colegas de turma, Gabriela, Luciano, Marcos e Wesley, pelas muitas risadas e por tornarem essa caminhada muito mais leve.

Aos amigos, Felipe e João, pelas nossas "pouquíssimas" horas de estudo coletivo.

RESUMO

MELO, Clarissa Duarte Loureiro de. *Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes*. 2014. 53 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional / PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2014.

Esta dissertação apresenta uma proposta para trabalhar Matrizes no Ensino Médio, a partir do exemplo de sua aplicação em Criptografia. A Cifra de Hill é o método criptográfico descrito e sugerido para realizar a construção dos conceitos de Matrizes. O objetivo é oferecer aos professores e aos licenciandos de Matemática um material que os ajude a realizar experiências semelhantes em suas salas de aula, na busca da superação do constante desafio que é promover o ensino e a aprendizagem de Matemática contextualizados, vinculados sempre que possível ao desenvolvimento científico e tecnológico. A Criptografia pode ser um excelente instrumento para alcançar esse objetivo. Ela mostra como a introdução da Matemática na construção de seus processos acelerou e promoveu o seu desenvolvimento e os reflexos desse desenvolvimento na sociedade ao longo da história.

Palavras-chave: Matrizes (Matemática) - Estudo e ensino. Criptografia. Matemática (Ensino Médio).

.

ABSTRACT

MELO, Clarissa Duarte Loureiro de. *Cryptography in High School: a proposal for teaching arrays.* 2014. 53 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional / PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2014.

This dissertation presents a proposal to work Matrices in High School, using the example of their application in Cryptography. The cryptographic method described and suggested for building up the concept of Matrices is the Hill Cipher. The objective is to offer to Mathematics teachers, and those studying to become teachers, material that will help them develop similar experiences in their classrooms, to overcome the constant challenge of promoting a contextualised Mathematics teaching and learning process, connected whenever possible to the course of scientific and technological development. Cryptography can serve as an excellent tool in this pursuit. It demonstrates how the introduction of Mathematics in the construction of cryptographic processes accelerated and promoted its development and the consequences of this development on society throughout history.

Keywords: Cryptography. Matrices. High School. Hill Cipher.

SUMÁRIO

INTRODUÇÃO

Ao optar por cursar um Mestrado Profissionalizante voltado para o Ensino de Matemática, certamente o Professor da disciplina tem por objetivo rever, aprender e aprofundar conhecimentos que lhe permitirão melhorar a sua prática docente.

Ensinar Matemática transcende a mera transmissão de conteúdos. Significa permitir que o aluno acesse um universo de conjecturas, reflexões, modelagens, cálculos, validações, resultados. Mesmo que o nosso sistema de ensino ainda conduza à realização de práticas tradicionais, é possível e necessário que o professor de Matemática da Educação Básica busque situações que lhe traga elementos capazes de gerar uma prática docente e discente pautada nos aspectos citados acima.

Diante dessa perspectiva, este trabalho apresenta a proposta de utilizar a Criptografia como tema a orientar uma prática de ensino de Matemática no Ensino Médio. A princípio, pode parecer inviável realizar tal proposta, levando em consideração essa etapa de formação escolar dos alunos. Afinal, os conceitos matemáticos que envolvem a criptografia atual são muito avançados para os alunos desse nível.

Todavia, a pesquisa realizada mostrou ser possível apresentar noções de Criptografia utilizando conceitos tradicionalmente ensinados no Ensino Médio (Matrizes, Determinantes e Sistemas Lineares, por exemplo) e, ainda, introduzir as noções elementares da Aritmética Modular nesse nível. Para completar a proposta, aspectos que envolvem o desenvolvimento da Criptografia ao longo da história da humanidade foram inseridos, de modo a oferecer um referencial de contextualização para o professor.

A Criptografia possui uma vasta área de aplicações no mundo contemporâneo. Não existe transação financeira que seja feita sem o seu emprego. Segredos de Estado são mantidos, via encriptações das informações sigilosas. Até o simples envio de uma mensagem, via e-mail, envolve um processo criptográfico. Na verdade, como será visto adiante, ela se faz presente na vida do homem, desde muito cedo.

O capítulo 1 deste trabalho apresenta alguns episódios que narram os primórdios da Criptografia e daquela que é sua rival e, ao mesmo tempo, a razão de seu constante aperfeiçoamento – a Criptoanálise. Além disso, explica o conceito de cifra, elemento primordial para a criação de um criptograma, e exemplifica algumas das cifras que marcaram momentos da humanidade. O capítulo encerra apresentando uma síntese da importância da mecanização dos processos de cifragem e decifragem, que abriram caminho para a era atual que caracteriza a criptografia digital.

O capítulo 2 realiza o tratamento matemático necessário à discussão do processo criptográfico sugerido para ser trabalhado em sala de aula: a Cifra de Hill. Nele serão apresentados os conceitos elementares da Álgebra Linear e Aritmética Modular necessários à compreensão da referida cifra. Evidentemente que o professor ao aderir a essa proposta

precisará adequar a linguagem, de acordo com seu público-alvo.

O capítulo 3 descreve todo o processo criptográfico que envolve a Cifra de Hill, desde a cifragem até decifragem. Menciona também os aspectos que caracterizam a sua fragilidade. Exemplos permeiam as explicações dos conceitos, facilitando a compreensão do processo.

O capítulo 4 apresenta uma breve descrição de uma experiência de aplicação da proposta apresentada nos capítulos anteriores. Ela foi realizada com um grupo de alunos, que na época cursavam o segundo ano do Ensino Médio em uma instituição de ensino particular do município do Rio de Janeiro. Foi através dessa vivência que a possibilidade de concretizar a proposta de prática docente sugerida nesse trabalho tornou-se realidade.

Encerrando este trabalho, seguem algumas observações e sugestões sobre a implementação da proposta apresentada, no intuito de orientar aqueles colegas que aceitarem o desafio de experimentar ensinar Matemática, através de caminhos menos ortodoxos e que valorizam os aspectos essenciais do verdadeiro significado de aprender e reconhecer a sua aplicação nos mais variados contextos.

1 CRIANDO E DESVENDANDO SEGREDOS

> "Nos seus quase quatro mil anos de história, a criptografia sofreu grandes transformações e também atuou como agente transformador. Conflitos armados, interesses comerciais, intolerância dos poderes constituídos, enfim, as situações de tensão e de perigo, a busca de lucro e a necessidade de poder que sempre fizeram parte da história impulsionaram e ainda impulsionam constantemente a evolução da criptografia". (TKOTZ, 2005)

"O segredo é a alma do negócio". Ditado popular muito conhecido, ele reitera a importância de preservar a confidencialidade das informações para o alcance de certos propósitos (empresariais, financeiros, políticos, militares, pacíficos ou não). Consequentemente, isso implica na criação de protocolos seguros que garantam a manutenção do sigilo dessas informações, principalmente no caso de possíveis interceptações durante a sua transmissão.

Desde a antiguidade, a preocupação em manter o caráter confidencial das informações durante as suas comunicações motivou o desenvolvimento e o aperfeiçoamento de técnicas que evitassem a revelação de seus conteúdos, caso as mensagens fossem indesejavelmente interceptadas. Os registros históricos apontam para a esteganografia (do grego "steganos": coberto; "graphein": escrever) como uma das primeiras técnicas utilizadas pela humanidade para promover a segurança na comunicação secreta da informação. Ela consiste na ocultação da existência da informação, através de algum meio físico ou químico. Apesar de muito empregada em várias épocas, ela oferece um nível de segurança muito baixo. Uma vez descoberto o processo de ocultação empregado, seu conteúdo será exposto e imediatamente conhecido por seus interceptadores.

Singh (2005) exemplifica alguns casos do uso da esteganografia para transmissão de informações sigilosas e que ilustram a fragilidade do método. Entre eles, dois relatos narrados por Herótodo, considerado o "pai da História". No primeiro, ocorrido no século V a.C., os gregos evitaram o ataque surpresa dos persas ao seu território, graças a uma mensagem enviada por Demarato, um grego exilado na Pérsia, mas leal à sua pátria. Para ocultar o conteúdo da mensagem, ele providenciou dois pares de tabuletas, raspou a cera sobre elas, escreveu a mensagem avisando sobre o plano de invasão persa e, por fim, os recobriu novamente com cera. A mensagem chegou a salvo ao seu destino e assim, em 480 a.C., quando os persas tentaram invadir as terras inimigas, foram os gregos que os surpreenderam e os derrotaram, garantindo a sua soberania.

No outro, narra a técnica que consistiu na raspagem da cabeça de um mensageiro e no registro da mensagem em seu couro cabeludo. Após o crescimento do cabelo, o mensageiro dirigiu-se ao seu destino sem sofrer qualquer tipo de interceptação, raspou novamente a cabeça e revelou o conteúdo da mensagem para o destinatário.

No século XVI, o cientista italiano Giovanni Porta descreveu uma técnica esteganográfica na qual era possível *"esconder uma mensagem dentro de um ovo cozido fazendo uma tinta com uma onça de alume e um quartilho de vinagre e então escrevendo na casca do ovo. A solução penetra na casca porosa e deixa a mensagem sobre a clara endurecida do ovo. Para ler basta retirar a casca o ovo."* (SINGH, 2005, p.21-22). Outras técnicas esteganográficas utilizaram o emprego de tinta invisível e foram empregadas, inclusive por espiões em pleno século XX.

O micropontо foi uma forma de esteganografia muito usada pelos alemães ao longo da Segunda Guerra Mundial para a transmissão de mensagens secretas. Consistia na redução fotográfica de uma página de texto, até a obtenção de uma imagem circular com diâmetro inferior a um milímetro. Em seguida, essa imagem circular era ocultada sob o ponto final de uma carta supostamente inofensiva e enviada ao seu destinatário. Tal prática obteve sucesso até 1941, quando o FBI foi alertado sobre a técnica empregada e passou a interceptar os micropontos, desvendando o conteúdo da maioria das mensagens neles contidas.

A vulnerabilidade da esteganografia, apesar do certo grau de evolução alcançado ao longo dos séculos, deu margem ao desenvolvimento, em paralelo, de outro método de proteção da informação: a criptografia (do grego "kriptos": oculto; "graphein": escrever). Ao contrário da esteganografia, a criptografia não pretende ocultar a informação contida em uma mensagem. Seu objetivo é tornar o significado da mensagem incompreensível para o caso de eventuais interceptações, assegurando maior grau de segurança da informação vinculada.

Segundo Singh (2005), foi através do uso combinado de técnicas esteganográficas e criptográficas que os americanos voltaram a ter problemas em obter informações de alguns micropontos alemães interceptados.

Se por um lado o surgimento da criptografia elevou o nível de segurança da informação, a busca por meios que permitissem burlar essa segurança também cresceu. Dessa necessidade surgiu a criptoanálise. Criptografia e criptoanálise são dois ramos de uma ciência que estuda a escrita secreta em todas as suas formas: a criptologia.

Este capítulo não tem a pretensão de discorrer sobre todos os aspectos que envolvem a história e evolução da criptografia e da criptoanálise. Na verdade, isso seria impossível. Além de se tratar de duas áreas do conhecimento em permanente aperfeiçoamento, ainda existe o fato de sua criação e aplicação possuir um caráter extremamente sigiloso. Muitos aspectos da evolução dos sistemas criptográficos e criptoanalíticos só vieram a público muito recentemente e tantos outros permanecem desconhecidos da grande maioria, restritos apenas a um seleto grupo responsável por seu desenvolvimento.

Na verdade, a intenção é apresentar conceitos elementares sobre essas duas áreas da criptologia, além de referências sobre alguns registros históricos que permitam orientar futuras práticas docentes voltadas para percepção da importância da contextua-

lização histórica e social que permeiam o desenvolvimento e aplicação do conhecimento matemático.

1.1 **A Criptografia e suas cifras**

O processo de encriptação de uma mensagem inicia-se a partir da cifragem do texto que contém a informação que deve ser transmitida. Chama-se cifra, à técnica que consiste na substituição de cada letra ou caracter da mensagem original por outras que foram retiradas de um alfabeto cifrado. Esse alfabeto cifrado é obtido através do rearranjo do alfabeto original.

Cada cifra é composta por um algoritmo e por uma chave. O algoritmo engloba os procedimentos de cifragem de uma mensagem. Segundo Couto (2008), é qualquer sistema geral, invariável e não ambíguo de instruções que permita transformar uma mensagem original em uma mensagem cifrada. A chave, por sua vez, é o elemento ou método específico que permitirá a decifragem da mensagem. Ela define qual o alfabeto cifrado será utilizado na cifragem/decifragem. A segurança de uma informação criptografada depende exclusivamente da preservação do sigilo em torno da chave.

As cifras podem ser classificadas em cifras de transposição e cifras de substituição.

1.1.1 Cifra de Transposição

A cifra de transposição é um sistema no qual cada caracter da mensagem original mantém sua identidade, apesar de ter sua posição trocada no texto cifrado. Essa troca resulta na obtenção de anagramas. Desta forma, se o número de letras da mensagem for aumentado, maior será o número de anagramas gerados e, portanto, maior será o nível de segurança oferecido.

Se por um lado a possibilidade de gerar um número muito grande de anagramas é vantajosa em relação à preservação do sigilo da mensagem, também há o risco da geração de um anagrama muito difícil. Esse fato aliado à falta de um protocolo adicional estabelecido entre emissor e receptor pode tornar a decifragem impossível até mesmo para o destinatário.

Um exemplo de uma cifra de transposição sistemática, isto é, onde um protocolo de cifragem e decifragem é estabelecido entre o remetente e o destinatário foi utilizado num dispositivo chamado Citale Espartano ou Bastão de Licurgo, figura (1). Esse dispositivo é reconhecido como o primeiro aparelho criptográfico militar e teria sido utilizado pela primeira vez durante o século V a.C. De acordo com Singh (2005), tratava-se de um bastão de madeira em volta do qual era enrolada uma tira de couro ou pergaminho. O

Figura 1 - Citale Espartano

remetente escrevia a mensagem ao longo do comprimento do dispositivo e, ao desenrolar a tira, a mensagem se desfazia em um emaranhado de letras sem sentido. Para decifrar a mensagem, o destinatário enrolava a tira em torno de um Citale que devia possuir o mesmo diâmetro do utilizado no processo de cifragem.

1.1.2 Cifra de Substituição

A cifra de substituição é um sistema no qual cada caracter da mensagem original é substituído por outro diferente, de forma que a sua identidade seja modificada, mas sua posição dentro da mensagem seja mantida.

Assim, no caso das cifras de substituição, substituir cada caracter do alfabeto original por outro do alfabeto cifrado constitui o algoritmo da cifra. Por sua vez, a chave definirá qual o alfabeto cifrado adequado a ser usado para a decifragem, dentre os diversos gerados pelo rearranjo do alfabeto original. O nível de segurança de uma cifra de substituição cresce à medida que se considera qualquer rearranjo do alfabeto original.

Em virtude de ser de fácil implementação e por proporcionar aparentemente um alto nível de segurança, a cifra de substituição prevaleceu como método de comunicação secreta confiável durante todo primeiro milênio da era cristã. Acreditava-se mesmo que seria indecifrável, até que por intermédio de uma combinação entre linguística, estatística e religiosidade, os árabes, em plena era de ascenção científica e cultural, encontraram um atalho no processo de busca pela chave correta. Esse atalho permitiu que uma mensagem fosse decifrada em minutos, ao invés dos bilhões de anos supostamente estimados por séculos. Mais adiante, será visto como se processou a "quebra" desta cifra, através de um processo conhecido como análise de frequências.

As cifras de substituição podem ser classificadas como monoalfabéticas e polial-

fabéticas. Enquanto nas cifras de substituição monoalfabéticas o alfabeto cifrado permanece fixo durante toda a cifragem, nas polialfabéticas o alfabeto cifrado muda durante a cifragem. Essa mudança é definida por uma chave.

Conforme mencionado anteriormente, no processo de cifragem por substituição polialfabética, vários alfabetos, de mesma origem ou não, são utilizados para realizar a substituição de um mesmo texto. Para obter um número ainda maior de alfabetos basta trocar as posições das letras de cada um.

A seguir, serão exemplificadas algumas cifras de substituição que se destacaram ao longo da história da evolução da criptografia.

- **A Cifra de César**

  A cifra de César, frequentemente citada em textos históricos sobre criptografia, é uma cifra de substituição monoalfabética. Recebeu esse nome por ser muito utilizada pelo imperador romano Júlio César, que para cifrar mensagens substituía cada letra da mensagem original por outra que estivesse três casas a sua frente.

  Exemplo:

c	i	f	r	a		d	e		c	e	s	a	r	(texto original)
F	L	I	U	D		G	H		F	H	V	D	U	(texto cifrado)

  O nível de segurança da cifra de César é muito fraco. O processo conforme usado por ele dispõe de apenas 25 chaves em potencial. Apesar disso, a cifra de César continuou sendo usada por muitos séculos.

  Entretanto, se considerarmos a formação de todo alfabeto cifrado a partir de qualquer rearranjo do alfabeto original, é possível gerar um número bem maior de chaves em potencial e com isso aumentar significativamente o nível de segurança desse processo de cifragem.

- **A Cifra de Vigenère**

  De acordo com Couto (2008), a cifra de Vigenère foi criada em 1553 e apesar de sua autoria ser atribuída a Blaise de Vigenère, o seu real criador teria sido Giovan Batista Belaso. Singh (2005), por sua vez, afirma que o nome atribuído à essa cifra seria uma homenagem à Blaise de Vigenère, responsável pelo aperfeiçoamento dos trabalhos anteriores de Alberti, Trithemius e Porta, todos criptógrafos cujas contribuições foram importantes para o desenvolvimento da criptografia.

  Trata-se de uma cifra de substituição polialfabética. É criada a partir de um alfabeto original e vinte seis alfabetos cifrados distintos que formam o chamado Quadrado de Vigenère, figura (2). Cada alfabeto cifrado é formado pelo deslocamento de uma letra para esquerda em relação ao alfabeto anterior.

Figura 2 - O quadrado de Vigenère

Alfabeto correto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A cifragem de cada letra do texto original é feita utilizando alfabetos cifrados diferentes localizados nas linhas do quadrado. Isto permite que uma mesma letra do texto original seja cifrada de formas diferentes. Assim, é necessário que remetente e destinatário conheçam previamente o sistema adotado para a mudança entre as linhas, através de uma palavra-chave.

Apesar de oferecer um nível de segurança muito alto, por conta de sua natureza polialfabética, seu emprego torna-se mais complicado, razão pela qual esse sistema acabou sendo negligenciado por quase dois séculos.

- **Cifra de Playfair**

  Criada por Sir Charles Wheatstone, mas publicada e popularizada por seu amigo Lyon Playfair, esta cifra utiliza uma matriz composta por letras e chaves. Caracteriza-se pela substituição de cada par de letras na mensagem original por outro par de letras. É necessário, no entanto, que o remetente e o destinatário estabeleçam uma palavra-chave para o pleno sucesso na recepção e compreensão da mensagem. Era considerada fácil e apropriada para campos de batalha.

  A cifra de Playfair é uma cifra de blocos primitiva que usa alguns princípios comuns às cifras de bloco atuais.

- **Cifra ADFGVX**

  É uma cifra caracterizada por elementos de transposição e substituição e foi amplamente empregada pelo exército alemão no período da I Guerra Mundial. As letras que nomeiam esta cifra compõe o texto cifrado.

  Exemplos de cifragem utilizando as cifras de Vigenère, Playfair e ADFGVX podem ser encontrados em Couto (2008) e Singh (2005).

- **Cifra de Hill**

  A cifra de Hill é uma cifra de substituição em blocos. Isto é, faz a encriptação das informações em blocos de tamanho fixo. Apesar de ser baseada em Álgebra Linear, implica também no uso de Aritmética Modular. Foi desenvolvida pelo criptógrafo norte americano Lester S. Hill e publicada em seu livro *Cryptography in na Algebraic Alphabet*, em 1929.

  No capítulo 3 desta dissertação, os processos de cifragem e decifragem que envolvem a aplicação da cifra de Hill serão descritos detalhadamente e exemplificados.

1.2 Criptografia e Criptoanálise: ciências rivais ou complementares?

Apesar do objetivo central deste trabalho ser a abordagem da criptografia, através de um processo de cifragem que envolve conceitos matemáticos, não é possível falar de criptografia sem mencionar a criptoanálise. Essas duas áreas da criptologia, ao mesmo tempo que travam uma batalha constante para uma sobrepor-se à outra, elas se complementam e fornecem elementos constantes para os seus aperfeiçoamentos.

Se para o criptógrafo o sucesso de seu trabalho reside na criação de mecanismos de cifragem que impeçam a quebra do sigilo de informações confidenciais durante sua transmissão, para o criptoanalista o sucesso é obtido quando vunerabilidades são encontradas nesses mecanismos e, então, os mesmos são compreendidos e o conteúdo criptografado é revelado.

Os árabes são considerados os grandes responsáveis pelo nascimento da ciência da Criptoanálise. Eles "quebraram" a cifra de substituição monoalfabética, invulnerável durante muitos séculos, conforme já mencionado. Em particular, grande destaque é atribuído a Al-Kind, que no século IX d.C. teria desenvolvido a técnica de decifragem conhecida como análise de frequências. Essa técnica consiste na comparação entre a frequência dos caracteres que aparecem em uma mensagem e a frequência em que os mesmos aparecem na língua na qual a mensagem foi escrita. Para isso, é preciso estudar vários textos na língua em questão e verificar com que frequência cada letra do alfabeto tende a aparecer.

Em seguida, a mensagem cifrada é analisada e os caracteres de maior frequência nela são destacados e associados aos caracteres de maior frequência na referida língua como seus prováveis correspondentes. A análise de frequências torna desnecessária a verificação de cada uma das muitas chaves em potencial. Favorece, ainda, a decifração de textos mais longos, uma vez que estes possuem maior probabilidade de fidelidade às frequências tidas como padrão.

Outro avanço relevante obtido pela Criptoanálise foi a quebra da cifra de Vigenère, em meados do século XIX. Ele é atribuído a Charles Babbage e Friedrich W. Kasiski e foi realizado em trabalhos independentes. Por ser uma cifra de substituição polialfabética, a cifra de Vinegère é imune à aplicação direta da técnica criptoanalítica de análise de frequências. Todavia, sua fraqueza está em sua natureza cíclica. Caso sua palavra-chave seja identificada, basta que o criptoanalista verifique o seu comprimento "n", que normalmente é pequeno, e tratar o texto cifrado como n cifras de substituição monoalfabéticas, empregando a análise de frequências para cada uma delas.

Mas foi no século XX, em função das duas Grandes Guerras Mundiais, que a criptoanálise deu um grande salto qualitativo e acirrou a competitividade entre criptógrafos e criptoanalistas.

O advento do rádio e seu uso na transmissão de mensagens durante a I Guerra Mundial intensificaram a necessidade de cifragens cada vez mais seguras. Afinal, se as comunicações haviam sido facilitadas, o mesmo ocorria com as interceptações das mesmas.

Apesar dessa necessidade urgente, de acordo com Singh (2005), o período de 1914 a 1918, que compreende o primeiro grande conflito de dimensões mundiais, caracterizou-se por uma sequência de fracassos criptográficos. Esses fracassos ocorreram por conta das fragilidades das cifras empregadas, que na verdade eram variações ou combinações de cifras anteriormente quebradas no século XIX.

Um exemplo dessa fragilidade foi a introdução da cifra ADFGVX pelos alemães no início de 1918. Eles confiavam demasiadamente na força oferecida por ela, em virtude de ser constituída por elementos de transposição e substituição. Todavia, três meses depois de sua implementação, ela foi quebrada pelo criptoanalista francês Georges Paivin, quando os alemães estavam próximos a Paris preparando-se para a ofensiva final.

A propósito, uma das qualidades que fizeram os franceses sobreporem-se aos alemães na I Guerra Mundial foi exatamente a preocupação que tiveram em desenvolver suas habilidades criptoanalíticas, desde o princípio do conflito. Os alemães, por sua vez, só vieram a criar um departamento criptoanalítico dois anos após o início da guerra.

Durante a I Guerra Mundial pode-se dizer que os criptoanalistas derrotaram os criptógrafos. Além dos franceses, considerados os mais eficientes criptoanalistas dos tempos de guerra, britânicos e americanos também somaram forças e juntos os aliados puderam sobrepor-se aos alemães.

Um exemplo clássico dessa supremacia aliada é ilustrado na decifração do telegrama

de Zimmermann, em 1917 (Singh, 2005). Arthur Zimmermann era Ministro de Relações Exteriores da Alemanha e havia orquestrado um plano que culminaria na rendição das forças aliadas e no impedimento da entrada dos EUA na guerra, que até então mantinham-se neutros.

Os aliados também se preocupavam com a produção de processos de cifragem seguros. O melhor exemplo foi a criação do Bloco de Cifras de Uma Única Vez pelos americanos, considerado o Santo Graal da criptografia. O nível de complexidade empregado nesse método é tão grande que o torna indecifrável, conforme já provado matematicamente. Ele consiste na criação de uma chave aleatória formada por letras dispostas ao acaso como parte da cifra de Vigenère. Segundo Singh (2005), o fato da chave ser aleatória gera um texto cifrado desprovido de padrões e estruturas nos quais os criptoanalistas possam se apoiar para decifrá-lo.

O sistema é composto por um bloco contendo centenas de folhas de papel. Cada uma dessas folhas possui uma chave aleatória única, de mesmo comprimento da mensagem e composta por linhas e letras dispostas numa sequência aleatória e que são parte da cifra de Vigenère. Remetente e destinatário recebem as duas únicas cópias do bloco. Cada folha do bloco é usada para cifragem e decifragem, através da aplicação da cifra de Vigenère e em seguida destruída, de modo a assegurar que nunca mais será utilizada.

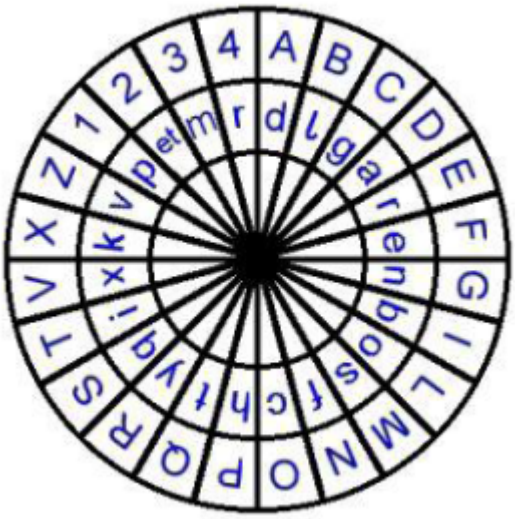
Apesar do nível de segurança inigualável, essa técnica apresentou desvantagens práticas em sua aplicação na guerra e por isso não foi empregada. Ela requeria a produção de um número muito grande de chaves aleatórias em função da necessidade da transmissão das muitas mensagens e a logística existente na época não era suficiente, além dos elevados custos que compreenderia.

O *Bloco de Cifras de Uma Única Vez* torna-se prático quando restringe-se à comunicações ultrassecretas, que dispõe de recursos logísticos e financeiros para tal. Um exemplo de utilização dessa técnica de cifragem estaria presente no famoso telefone vermelho utilizados pelos presidentes dos EUA e Rússia.

Não só de inteligência, papel e lápis a história da criptografia e da criptoanálise foi construída. Dispositivos mecânicos e eletromecânicos foram projetados, criados e aperfeiçoados para que tornassem o processo de cifragem e decifragem mais rápidos e práticos. Dois deles foram o disco de Alberti e a máquina Enigma.

O disco de cifras ou disco de Alberti, figura (3) é considerado a primeira máquina criptográfica. É uma versão mecanizada da cifra de Vigenère. Foi inventado no século XV pelo arquiteto italiano Leon Alberti, um dos responsáveis pelo desenvolvimento da cifra de substituição polialfabética que, conforme visto anteriormente, permite que diferentes caracteres cifrados possam representar o mesmo caracter do texto claro, o que dificulta a interpretação pela análise de frequências.

Figura 3 - Disco de Alberti



Segue a descrição de COUTO (2008, p. 76) sobre o referido dispositivo:

> "... um sistema de encriptação que usava dois discos concêntricos de metal cujas circunferências eram divididas em 24 partes iguais. Os segmentos do disco externo continha as letras do alfabeto em ordem randômica(menos as letras h, k e y, além das letras que não havia no alfabeto latino, como j, u e w) e números de 1 a 4.
> Para enviar uma mensagem criptografada, as letras ou números de um texto claro eram lidas no disco externo e substituídas pelas correspondentes à mesma posição no disco interno. A pessoa que enviava e a que recebia deveriam ter o mesmo disco."

A Enigma da figura (4) foi a mais importante máquina de cifragem empregada ao longo da Segunda Guerra Mundial. Versão eletromecânica do disco de Alberti, ela foi inventada pelo engenheiro alemão Arthur Scherbius, em 1918. Inicialmente adotada apenas para uso comercial, tão logo as vantagens que imprimia à segurança da informação foram conhecidas, foi devidamente adaptada e usada apenas pelas forças militares alemães. Nas duas décadas seguintes que sucederam a sua criação, cerca de trinta mil Enigmas foram compradas pelos militares alemães. De acordo com Singh (2005), no início da Segunda Guerra as comunicações alemães contavam com uma proteção em seus sistemas de informação inigualável, em virtude do alto nível de cifragem oferecido pela Enigma.

Figura 4 - Enigma

De modo bem simplificado, pode-se dizer que a Enigma era composta por três elementos ligados por fios. Em um teclado eram digitadas cada letra do texto original. A cifragem era feita por intermédio de uma unidade misturadora, a parte mais importante da máquina, cujo aperfeiçoamento ao longo dos anos foi tornando a Enigma uma das principais armas daquela Guerra. A força da cifra gerada por ela dependia do ajuste inicial desses misturadores. Por fim, havia um mostrador composto por várias lâmpadas que indicavam as letras do texto cifrado.

Para decifrar a mensagem, o destinatário deveria possuir outra máquina Enigma e um livro contendo informações sobre o ajuste inicial dos misturadores utilizado para aquele determinado dia.

Apesar de ter sido largamente empregada na transmissão de informações sigilosas que permitiram o avanço alemão e quase vitória durante a Segunda Guerra, a decifragem do funcionamento da Enigma começou muitos anos antes, ainda no período entre guerras.

Em 1931, um alemão chamado Hans-Thilo Schmit traiu sua pátria (e quem sabe

salvou o mundo!) vendendo à França fotografias de dois documentos que continham instruções sobre o funcionamento da Enigma. Com base nesses documentos foi construída uma réplica da Enigma e iniciado um longo processo de pesquisa sobre o seu funcionamento.

Entretanto, ter apenas uma réplica da Enigma não era suficiente para decifrar as mensagens alemães. Era preciso conhecer a chave e esta dependia do conhecimento dos ajustes iniciais da máquina. Os franceses não acreditavam numa nova ofensiva alemã e não se esforçaram o suficiente para decifrar a Enigma. Julgavam mesmo ser impossível. Porém, passaram todas as informações obtidas, via espionagem, para os poloneses que, ao contrário deles temiam por nova invasão alemã ao seu território.

Os poloneses possuíam um departamento devotado à decifragem de mensagens em busca de potenciais sinais de ameaça à sua soberania, o Biuro Szyfrów. A partir dos primeiros contatos com a natureza da Enigma, eles peceberam que era preciso renovar o perfil dos criptoanalistas, que até então era formado por peritos em estrutura de linguagem. Se a Enigma produzia uma cifra mecânica, era preciso contar com mentes científicas para poder ajudar na sua decifração. Assim, o Biuro recrutou vinte matemáticos e promoveu um curso de criptografia sob sigilo. Somente três matemáticos foram considerados aptos e passaram a trabalhar no departamento. Entre eles estava Marian Rejewski, o responsável direto pelas primeiras decifragens das cifras produzidas pela Enigma. De forma bastante simplificada, pode-se dizer que o sucesso do trabalho de Rejewski residiu no fato da percepção de repetições no processo de cifragem que permitiram o reconhecimento de padrões. A compreensão sobre esses padrões permitiu que ele produzisse um catálogo que lhe conduzia a descoberta da chave diária. Singh (2005) afirma que a decifragem da Enigma foi umas das grandes realizações na história da criptoanálise.

Mesmo quando os alemães fizeram alterações no funcionamento da Enigma, em 1934, Rejewski conseguiu fazer as adaptações necessárias e produziu as primeiras versões mecanizadas da criptoanálise: as Bombas. Essas máquinas de decifragem eram capazes de verificar automaticamente os ajustes corretos dos misturadores da Enigma. Cada Bomba era composta por seis dispositivos que funcionavam em paralelo e juntos formavam uma unidade de quase um metro de altura.

Apesar da genialidade e esforço constante de Rejewski em ajustar suas máquinas em função das modificações implementadas pelos alemães na Enigma, a partir de 1939 nada mais ele pôde fazer. O requinte de aperfeiçoamento da Enigma exigia mais do que esforço intelectual. Demandava também tempo e dinheiro para construção de novas Bombas, o que a Polônia não dispunha mais. Prevendo a inevitável invasão de seu território e não querendo que os avanços obtidos por Rejewski caíssem em mãos inimigas, o diretor do Biuro, Major Langer, convidou franceses e britânicos a uma visita à Varsóvia. Nela, revelou para os criptoanalistas presentes, em meio à incredulidade e surpresa destes, todo trabalho produzido por Rejewski e sua equipe em pouco menos de dez anos. Para finalizar

ainda ofereceu aos britânicos e franceses duas réplicas sobressalentes da Enigma e todas as plantas e diagramas das Bombas. Pouco tempo depois, em 1º de setembro de 1939, a Polônia foi invadida pela Alemanha, dando início à Segunda Guerra Mundial.

A força bruta, como denominam os criptoanalistas, foi por muito tempo o único recurso que tinham para lidar com as mensagens cifradas. Inteligência e persistência eram as únicas armas contra o inimigo a ser vencido. A invenção da Enigma e o seu processo eletromecânico de cifragem chegaram a fazer crer que os criptoanalistas não teriam mais chances de sobrepor os criptógrafos. Porém, os avanços produzidos pelos poloneses, em particular com a criação das máquinas de decifragem de Rejewski, mostrou que a Enigma não era invulnerável. Mais ainda. Mostrou ser fundamental a presença de matemáticos e cientistas nas equipes de criptoanalistas, até então essencialmente formadas por linguistas e especialistas em clássicos.

Foi assim que o britânico Alan Turing, um dos maiores matemáticos do século XX, participou decisivamente do aperfeiçoamento do trabalho do matemático polonês Rejewski e criou novas Bombas capazes de decifrar as Enigmas alemães que se apresentavam cada vez mais sofisticadas durante a Segunda Guerra Mundial.

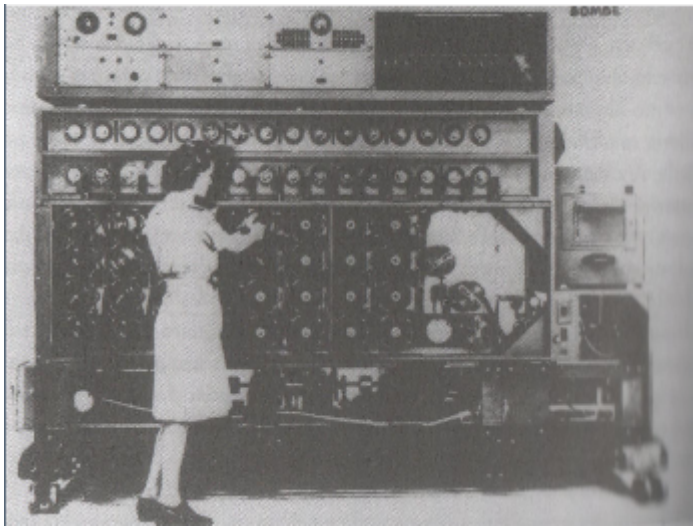
Turing já havia produzido um trabalho teórico sobre uma máquina capaz de solucionar qualquer questão que pudesse ser respondida pela lógica. Essa máquina imaginária, pois não havia tecnologia à época que permitisse a sua construção, foi batizada pelo próprio Turing como *máquina universal de Turing*. Anos mais tarde, os primeiros computadores foram concebidos a partir dela.

Embora suas teorias não pudessem ser postas em prática na época da concepção, o trabalho intelectual desenvolvido para elas foi muito útil quando passou a integrar o grupo de criptoanalistas da Escola de Cifras e Códigos do Governo Britânico, situada em Bletchley Park, na Inglaterra, em 1939. Turing identificou falhas humanas no processo de cifragem da Enigma que permitiram que desenvolvesse um sistema de decifragem que culminou na produção de novas Bombas que, apesar do nome, eram muito mais sofisticadas que as de Rejewski.

O primeiro protótipo da Bomba de Turing chamada de Victory ficou pronta em março de 1940, mas frustrou as expectativas iniciais. Era mais lenta do que se supunha e, portanto, precisou sofrer alguns ajustes. Logo em seguida, os alemães promoveram novos ajustes na Enigma, diminuindo muito a decifragem das mensagens. Finalmente em agosto de 1940, a nova Bomba de Turing estava pronta e desta vez correspondeu às expectativas. Foi batizada de Agnus Dei e apelidada de Agnes e em apenas dezoito meses outras quinze "Agnes" estavam funcionando a pleno vapor. Cada uma delas era capaz de decifrar uma chave da Enigma em cerca de apenas uma hora, o que permitia aos aliados decifrarem uma mensagem no mesmo dia em que era interceptada.

Se a máquina alemã Enigma representou um grande avanço técnico da criptografia para época, o britânico Colossus representou o primeiro grande avanço tecnológico em

Figura 5 - Bomba Turing



prol da criptoanálise.

Segundo Singh (2005), o Colossus foi a primeira máquina programável de que se tem registro, tornando-se o precursor do moderno computador digital. Ele foi projetado pelo matemático Max Newman, que trabalhava a serviço de Bletchley Park, e era capaz de se adaptar à resolução de diferentes problemas. Baseado em grande parte no conceito da máquina universal de Turing, possuía 1500 válvulas eletrônicas, o que imprimia maior velocidade de processamento comparado aos relés eletromecânicos das bombas de Turing. Foi graças ao Colossus que a cifra alemã Lorenz foi quebrada, tornando as comunicações entre Hitler e seus generais vulneráveis. Com o fim da Segunda Guerra Mundial, o Colossus e todos os registros de sua construção e operação foram destruídos, fato que fez com que sua existência ficasse oculta por muitos anos e permitisse que o ENIAC fosse considerado o primeiro computador programável da história.

Apesar de contraditório, uma vez que foi criado para acelerar o processo de decifragem, foi também a partir do Colossus que a criptografia abandonou a era da cifragem mecânica e entrou na era da cifragem digital, tornando a transmissão de informações muito mais rápida e segura.

Naturalmente, as contribuições da Matemática tornaram-se cada vez mais importantes para o desenvolvimento dos processos criptográficos e hoje a Teoria dos Números, assim como a Álgebra Linear são as áreas do conhecimento matemático que permeiam o seu desenvolvimento.

No próximo capítulo veremos alguns dos conceitos básicos dessas duas áreas da Matemática e que fundamentam a Cifra de Hill, um dos processos criptográficos desenvolvidos no início do século XX. A simplicidade conceitual que envolve essa cifra permite que ela seja trabalhada com alunos de Ensino Médio, conciliando o propósito de apresentar a aplicação prática de conhecimentos matemáticos e a construção desses conceitos,

através da criptografia.

2 ARITMÉTICA MODULAR E ÁLGEBRA LINEAR

Encontram-se no estudo da Cifra de Hill aplicações da Aritmética Modular e da Álgebra Linear. Neste capítulo será feita uma abordagem dos principais conceitos necessários ao estudo do método para melhor compreensão do leitor. Os teoremas e proposições enunciados no presente capítulo estão demonstrados na bibliografia deste trabalho. No intuito de facilitar a leitura, a referência bibliográfica utilizada, em cada caso, será devidamente indicada.

2.1 Máximo Divisor Comum

Definição 1: Dados dois números inteiros a e b, não simultaneamente nulos, diremos que o número inteiro $d \in \mathbb{N}^*$ é um *divisor comum* de a e b se $d|a$ (lê-se d divide a) e $d|b$ (lê-se d divide b).
Diz-se que d é um *máximo divisor comum* (mdc) de a e b se possuir as seguinte propriedades:

(i) d é um divisor comum de a e de b, e

(ii) d é divisível por todo divisor comum de a e b.

Segue da definição que o máximo divisor comum de dois números inteiros a e b (não ambos nulos) sempre existe e é único. Ele é denotado por $mdc(a, b)$.

Tem-se ainda a seguinte propriedade:

Se $d = mdc(a, b)$, então existem inteiros u e v (não necessariamente únicos) tais que $ua + vb = d$, onde esses u e v podem ser encontrados utilizando-se o Algoritmo Estendido de Euclides (AEE) conforme descrito em Coutinho (2009, p. 23-31)

Exemplo 1:Encontrar u e v, tais que $294u + 108v = mdc(294, 108)$.

Resto	Quociente	u	v
294	*	1	0
108	*	0	1
78	2	$1-2\cdot 0=1$	$0-2\cdot 1=-2$
30	1	$0-1\cdot 1=-1$	$1-1\cdot(-2)=3$
18	2	$1-2\cdot(-1)=3$	$-2-2\cdot 3=-8$
12	1	$-1-1\cdot 3=-4$	$3-1\cdot(-8)=11$
6	1	$3-1\cdot(-4)=7$	$-8-1\cdot 11=-19$
0	2		

Portanto $u=7$, $v=-19$ e $d=6$ e $294\cdot 7+108\cdot(-19)=6$.

Proposição 1: Sejam $a,b,c\in\mathbb{Z}$ com $b>1$.
$mdc(a,m)=mdc(b,m)=1$ se, e somente se, $mdc(a\cdot c,b)=1$.

Demonstração:

Se $mdc(ac,b)=1\Rightarrow\exists\ x,y\in\mathbb{Z}$ tais que, $acx+by=1\Rightarrow\begin{cases}a(cx)+by=1(i)\\c(ax)+by=1(ii)\end{cases}$. Se $d=mdc(a,b)\Rightarrow d|a,d|b$ e então por (i) segue que $d|1$, e portanto $d=1$. Analogamente, se $d'=mdc(c,b)$ segue por (ii) que $d'=1$. Logo, $d=d'=1$.

Para completar a demonstração, é necessário provar que se $mdc(a,b)=1$ e $mdc(c,b)=1$, então $mdc(ac,b)=mdc(c,b)$.

Seja $d=mdc(ac,b)$ e $d'=mdc(c,b)$.

Será mostrado que $d=d'$.

Como $d'|c$ e $d'|b\Rightarrow d'|ac$ e $d'|b\Rightarrow d'|d$.

Como $mdc(a,b)=1\Rightarrow\exists m,n\in\mathbb{Z}$ tais que, $am+bn=1\Rightarrow acm+bcn=c$. Como $d=mdc(ac,b)\Rightarrow d|ac$ e $d|b\Rightarrow d|c$. Logo, $d|b$ e $d|c\Rightarrow d|mdc(b,c)=d'$. Portanto $d|d'$ e então $d=d'$.

Portanto $mdc(ac,b)=mdc(c,b)$, e como $mdc(c,b)=1$ por hipótese, temos o resultado.

2.2 Aritmética Modular

Definição 1: Dados a, b e m inteiros quaisquer, com $m > 1$, dizemos que a é congruente a b módulo m, e escrevemos

$$a \equiv b \pmod{m}$$

se $a - b$ é um múltiplo inteiro de m.

Exemplo 1:

a) $73 \equiv 4 \pmod{23}$, pois $73 - 4 = 69$ é múltiplo de 23.

b) $21 \equiv -9 \pmod{10}$, pois $21 - (-9) = 30$ é múltiplo de 10.

c) $25 \equiv 0 \pmod{5}$, pois $25 - 0 = 25$ é múltiplo de 5.

Proposição 1: Seja m um inteiro positivo. Para todos $a, b, c \in \mathbb{Z}$, tem-se que

(i) $a \equiv a \pmod{m}$

(ii) se $a \equiv b \pmod{m}$ então $b \equiv a \pmod{m}$

(iii) se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Essas propriedades são decorrências imediatas da definição de congruência.

Conclui-se, dessa forma, que a congruência modular é uma relação de equivalência, visto que as propriedades descritas correspondem respectivamente à reflexão, simetria e transitividade. Todo número inteiro a é congruente módulo m a um, e somente um, dos inteiros $0, 1, ..., m - 1$. Estes números são chamados *classes de congruência* ou *resíduos* módulo m e formam o conjunto dos resíduos módulo m, representado por

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$$

.

Proposição 2: Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

(i) se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$

(ii) se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \cdot c \equiv b \cdot d \pmod{m}$.

Definição 2: Dado um número a em Z_m, dizemos que um número b em Z_m é um **recíproco** ou **inverso multiplicativo** de a módulo m se $a \cdot b \equiv b \cdot a \equiv 1 \pmod{m}$. Representa-se $b = a^{-1}$.

Exemplo 2: O número 3 possui inverso multiplicativo módulo 10. Ele pode ser obtido encontrando-se o valor de x em Z_{10}, tal que

$$3 \cdot x \equiv 1 \pmod{10}$$

$$3 \cdot 7 = 21 \equiv 1 \pmod{10}$$

portanto, $3^{-1} = 7 \pmod{10}$.

O resultado seguinte estabelece a condição necessária e suficiente para um inteiro ter ou não um recíproco.

Proposição 3: Seja $a \in \mathbb{Z}_m$ com $a \neq 0$ e $m > 1$. O número a é invertível módulo m se, e somente se, $mdc(a, m) = 1$.

O conjunto $U_m = \{a \in \mathbb{Z}_m | mdc(a, m) = 1\}$ de todos os elementos invertíveis em $\mathbb{Z}_m$ possui exatamente $\varphi(m)$ elementos (onde φ é a função de Euler).

Pela proposição 1 da seção 2.1 segue que U_m é fechado em relação à multiplicação e mais ainda, é um grupo abeliano.

Se $mdc(a, m) = 1$, a é invertível módulo m. Usando o Algoritmo Estendido de Euclides, é possível encontrar inteiros u e v tais que $au + mv = 1$. Daí,

$$au \equiv 1 \pmod{m} \text{ e portanto } a^{-1} = u \in U_m.$$

Para ilustrar a aplicação da proposição 3, o exemplo anterior será resolvido novamente.

Exemplo 3: Achar o recíproco de 3 módulo 10, caso exista.

Solução: Como $mdc(3, 10) = 1$, então o recíproco de 3 existe. É necessário então, determinar u e v tais que $3u + 10v = 1$. Neste caso, pelo Algoritmo Estendido de Euclides, $u = -3$ e $v = 1$.

Tem-se $3 \cdot (-3) + 10 \cdot 1 = 1$.

Na congruência módulo 10 a sentença acima pode ser reescrita como $3 \cdot (-3) + 0 \cdot 1 \equiv 1$, ou seja, $3 \cdot (-3) \equiv 1$.

Tabela 1 - Recíprocos Módulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

E, portanto, o recíproco de 3 módulo 10 é -3, que corresponde à classe do 7. Daí, $3^{-1} = 7$.

Em $\mathbb{Z}_m$ são definidas duas operações, adição "+"e multiplicação "$\cdot$"de tal forma que $(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo com identidade.

Como a Cifra de Hill utiliza as classes de congruência módulo 26, serão indicados todos os inversos multiplicativos nesse módulo para referência futura, tabela (1)

2.3 Matrizes e Aritmética Modular

Nesta seção será considerado o conjunto $M_n(R)$ das matrizes quadradas de ordem n com entradas num anel comutativo com identidade R. Embora R possa ser arbitrário, na maioria das vezes será o anel $\mathbb{Z}$ dos números inteiros ou o anel $\mathbb{Z}_m$ dos inteiros módulo m.

Definição 1: Uma matriz A_n com entradas em $\mathbb{Z}$ é uma tabela de n^2 elementos organizados em n linhas e n colunas

$$A_n = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix},$$

onde $a_{ij} \in \mathbb{Z}$ representa a entrada da linha i e coluna j de A_n.

Definição 2: Duas matrizes $A = (a_{ij})$ e $B = (b_{ij})$ em $M_n(\mathbb{Z})$ são ditas congruentes módulo m ($A \equiv B \pmod{m}$) se, e somente se, $a_{ij} \equiv b_{ij} \pmod{m}$, $\forall\ 1 \leq i, j \leq n$.

Os elementos a_{ij} em que $i = j$, formam a *diagonal principal* de A_n. Logo,

$$a_{11}, a_{22}, a_{33}, ..., a_{nn}$$

é a diagonal principal da matriz quadrada $A_n = (a_{ij})$.

Exemplo 1:

$$A = \begin{pmatrix} 2 & 29 & 100 \\ -5 & 51 & 10 \\ 4 & -3 & -40 \end{pmatrix} \equiv \begin{pmatrix} 2 & 3 & 22 \\ 21 & 25 & 10 \\ 4 & 23 & 12 \end{pmatrix} \pmod{26}$$

A diagonal principal é formada pelos elementos 2, 25 e 12.

Definição 3: *Matriz diagonal* de ordem n é toda matriz quadrada $n \times n$ cujos elementos fora da diagonal principal são iguais a zero. Isto é:

$A_n = (a_{ij})_{n\times n}$ é matriz diagonal se, e somente se, $a_{ij} = 0$ para cada $1 \leq i, j \leq n$ tais que $i \neq j$.

Dentre as matrizes diagonais temos a matriz identidade I_n na qual todos os elementos da diagonal principal são iguais a 1.

Exemplo 2:

a) $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

b) $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Definição 4: A *transposta* de uma matriz A, de ordem m por n é uma matriz, de ordem n por m, denotada por A^t, obtida pela permutação das linhas de A pelas suas colunas.

Exemplo 3:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}; \quad A^t = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{pmatrix}$$

Definição 5: Chama-se *matriz simétrica* toda matriz quadrada A, de ordem n, tal que $A^t = A$.

Decorre da definição que, se $A = (a_{ij})$ é matriz simétrica, tem-se:

$$a_{ij} = a_{ji}; \ \ \forall i, \forall j \in \{1, 2, 3, ..., n\}$$

isto é, os elementos simetricamente dispostos em relação à diagonal principal são iguais.

A seguir serão apresentadas as operações de adição e multiplicação de matrizes no conjunto $M_n(R)$, como também a multiplicação por escalar, que serão utilizadas ao longo deste trabalho.

Definição 6: *Adição de Matrizes*

A soma de duas matrizes A e B, de ordem n, é dada por uma matriz C, também de ordem n, obtida por

$$c_{ij} = a_{ij} + b_{ij}, \text{ para todo } i \text{ e para todo } j.$$

Definição 7: *Multiplicação de Matrizes*

Dadas duas matrizes A e B, de ordem n, chama-se produto AB à matriz $C = (c_{ik})$, de ordem n, tal que:

$$c_{ik} = a_{i1} \cdot b_{1k} + a_{i2} \cdot b_{2k} + ... + a_{in} \cdot b_{nk} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

para todo $i \in \{1, 2, ...n\}$ e todo $k \in \{1, 2, ..., n\}$

Importante: O produto AB existe somente se o número de colunas de A for igual ao número de linhas de B. Como o conjunto abordado é o de matrizes quadradas, essa condição é imediatamente satisfeita. Além disso, observa-se que o produto não é comutativo.

Definição 8: *Multiplicação de uma matriz por um escalar*
Se $k \in \mathbb{Z}$ (ou R) e $A \in M_n(R)$, então o produto $k \cdot A$ é a matriz $B = (b_{ij}) \in M_n(R)$, tal que:

$$b_{ij} = k \cdot a_{ij}.$$

Observação: Se $k \in \mathbb{Z}$ e $a \in \mathbb{R}$, então o produto $k \cdot a$ é dado por $a + a + ... + a$ (k vezes), onde $+$ é a adição do anel R.
Proposição 1: Se $A, B \in M_n(R)$ e $k \in \mathbb{Z}$ ou R, então $k(AB) = (kA)B = A(kB)$.

Essa definição se faz necessária, em virtude da propriedade sobre determinantes, que será vista mais adiante.

Ainda se faz necessário estabelecer as condições para que uma matriz A, de ordem n com entradas em $\mathbb{Z}$ seja invertível módulo m. Para isso, é preciso definir *determinante* e *matriz adjunta*.

Definição 9: Seja $A = (a_{ij})$ uma matriz no conjunto $M_n(R)$. Chama-se determinante da matriz A, e indica-se por $detA$, o número, em R que é obtido operando com os elementos de A da seguinte forma:

1º) Se A é de ordem 1, então $detA$ é o próprio elemento de A. Notação: $detA = a_{11}$.

2º) Se A é de ordem 2, tem-se que:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{e} \quad detA = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}.$$

3º) Se A é de ordem $n \geq 2$, então é possível calcular seu determinante através de *cofatores*.

O cofator do elemento a_{ij}, representado por Δ_{ij} é tal que $\Delta_{ij} = (-1)^{i+j} \cdot detA_{ij}$, em que A_{ij} é o determinante da submatriz que se obtém de A, eliminando sua i-ésima linha e j-ésima coluna.
Sendo,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

$$detA = a_{i1}\Delta_{i1} + a_{i2}\Delta_{i2} + \ldots + a_{in}\Delta_{in}$$
(expansão em cofatores pela linha i)
ou
$$detA = a_{1j}\Delta_{1j} + a_{2j}\Delta_{2j} + \ldots + a_{nj}\Delta_{nj}$$
(expansão em cofatores pela coluna j)

Exemplo 4: Se o determinante de A for calculado através da expansão em cofatores pela coluna 1, então,

$$detA = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{11} \cdot \Delta_{11} + a_{21} \cdot \Delta_{21} + \cdots + a_{n1} \cdot \Delta_{n1} = \sum_{i=1}^{n} a_{i1} \cdot \Delta_{i1}$$

Ou seja, o determinante é obtido somando-se os produtos da 1ª coluna pelos respectivos cofatores. Também poderia-se fixar qualquer outra linha ou coluna.

Teorema 1: Seja R um anel comutativo com identidade. Para matrizes $A, B \in M_n(R)$, $det(AB) = (detA) \cdot (detB)$.

Vide demonstração em Dummit (1999, p.419).

Definição 10: *Matriz dos Cofatores*
Seja A uma matriz de ordem n. Chama-se matriz dos cofatores de A, a matriz $A^{'}$ que se obtem substituindo cada elemento de A por seu cofator.

$$\text{Assim, se } A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \text{ então } A^{'} = \begin{pmatrix} \Delta_{11} & \Delta_{12} & \cdots & \Delta_{1n} \\ \Delta_{21} & \Delta_{22} & \cdots & \Delta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{n1} & \Delta_{n2} & \cdots & \Delta_{nn} \end{pmatrix}.$$

Definição 11: *Matriz adjunta* de A é denotada por $\bar{A}$ e consiste na transposta da matriz dos cofatores. Isto é, $\bar{A} = (A')^t$.

$$\bar{A} = \begin{pmatrix} \Delta_{11} & \Delta_{21} & \cdots & \Delta_{n1} \\ \Delta_{12} & \Delta_{22} & \cdots & \Delta_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{1n} & \Delta_{2n} & \cdots & \Delta_{nn} \end{pmatrix}$$

Observe que se $A \in M_n(R)$, então $\bar{A} \in M_n(R)$, pois cada cofator Δ_{ij} é um elemento de R.

Definição 12: Seja $A \in M_n(R)$. Dizemos que A é invertível se existir uma matriz $B \in M_n(R)$ tal que $A \cdot B = I_n$ e $B \cdot A = I_n$.

Quando tal matriz B existir, ela é unicamente determinada e é denotada por A^{-1}.

Teorema 2: (*Fórmula do Cofator para a Inversa de uma Matriz*) Seja $A \in M_n(R)$ e seja $\bar{A}$ a adjunta de A. Então, $A \cdot \bar{A} = \bar{A} \cdot A = (detA) \cdot I_n$. Além disso, $detA$ é invertível em R se, e somente se, A é invertível em $M_n(R)$; neste caso a matriz $\frac{1}{detA} \cdot \bar{A}$ é a inversa de A.

Vide demonstração em Dummit (1999, p. 420).

Corolário 1: Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, o $detA$ for invertível módulo m. Isto é, se, e somente se, $mdc(detA, m) = 1$.

Demonstração:

Suponha que $A \in M_n(\mathbb{Z}_m)$ seja invertível. Logo, existe $A^{-1} \in M_n(\mathbb{Z}_m)$ tal que $A \cdot A^{-1} = I_n$. Pelo Teorema 1 desta seção tem-se que $1 = det(I_n) = det(A \cdot A^{-1}) = (detA) \cdot (detA^{-1})$.
Logo $detA$ é invertível em $\mathbb{Z}_m$ e portanto $mdc(detA, m) = 1$.
Reciprocamente, suponha que $detA$ seja invertível em $\mathbb{Z}_m$. Então, existe $(detA)^{-1}$ em $\mathbb{Z}_m$ tal que $(detA) \cdot (detA)^{-1} = 1$. Do Teorema 2 acima e da Proposição 1 da seção 2.3, segue que:

$$A \cdot (detA)^{-1} \cdot \bar{A} = I_n.$$

Isto mostra que A é invertível e que $A^{-1} = \frac{1}{detA} \cdot \bar{A}$.

2.4 Conceitos Básicos de Álgebra Linear

No capítulo 3 são utilizados alguns conceitos da Álgebra Linear a nível de graduação. Entretanto, nesta seção, serão citados apenas as definições e propriedades necessárias à compreensão plena dos processos descritos posteriormente. Os espaços vetoriais serão $\mathbb{R}$ - espaços vetoriais de dimensão finita, onde $\mathbb{R}$ denota o corpo dos números reais.

Definição 1: Sejam V e W espaços vetoriais. Uma aplicação $T : V \longrightarrow W$ é chamada *transformação linear* de V em W se:

I) $T(u + v) = T(u) + T(v)$

II) $T(\alpha u) = \alpha T(u)$

para cada $u, v \in V$ e cada $\alpha \in \mathbb{R}$.

Observações:

a) Uma transformação linear de V em V é chamada *operador linear* sobre V.

b) Uma matriz $A_{m\times n}$ sempre determina uma transformação linear

$$T_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$$

onde a imagem $T_A(v) = Av$ é o produto da matriz A pelo vetor $v \in \mathbb{R}^n$ considerado como uma matriz de ordem $n \times 1$. Uma transformação linear desse tipo chama-se *multiplicação por A*.

c) Toda transformação linear $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ é determinada por uma matriz $A_{m\times n}$ tal que $T = T_A$, na qual A é dada por:

$$\Big(T(e_1) \quad T(e_2) \quad \dots \quad T(e_n)\Big)$$

sendo $e_1, e_2, \dots, e_n$ a base canônica de $\mathbb{R}^n$.
A é chamada a *matriz canônica* de T, e é geralmente denotada por $[T]$.

Exemplo 1: Se $A = \begin{pmatrix} 1 & 2 & -1 \\ 3 & 0 & 5 \end{pmatrix}$, então $T_A : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ é a transformação linear definida por $T_A(x, y, z) = (x + 2y - z, 3x + 5z)$.
Por outro lado, se $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ é a transformação linear definida por $T(x, y, z) = (x + y, 2x - y + 4z, y - z)$ então $[T] = \begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 4 \\ 0 & 1 & -1 \end{pmatrix}$ é a matriz canônica de T.

Propriedade: Se $T : V \longrightarrow W$ for uma transformação linear, então

$$T(a_1v_1 + a_2v_2) = a_1T(v_1) + a_2T(v_2)$$

$\forall v_1, v_2 \in V$ e $\forall a_1, a_2 \in \mathbb{R}$.

Indutivamente, tem-se:

$$T(a_1v_1 + a_2v_2 + ... + a_nv_n) = a_1T(v_1) + a_2T(v_2) + ... + a_nT(v_n)$$

$\forall v_i \in V$ e $\forall a_i \in \mathbb{R}, i = 1, 2, ..., n$, isto é, a imagem de uma combinação linear de vetores é uma combinação linear das imagens desses vetores, com os mesmos coeficientes.

Supondo que $v_1, v_2, ..., v_n$ seja uma base de V e que se saiba quais são as imagens $T(v_1), T(v_2), ..., T(v_n)$ dos vetores dessa base, sempre é possível obter a imagem $T(v)$ de qualquer $v \in V$, pois sendo v uma combinação linear dos vetores da base, isto é:

$$v = a_1v_1 + a_2v_2 + ... + a_nv_n$$

tem-se que:

$$T(v) = a_1T(v_1) + a_2T(v_2) + ... + a_nT(v_n)$$

Assim, uma transformação linear $T : V \longrightarrow W$ fica completamente definida quando se conhecem as imagens dos vetores de uma base de V.

Exemplo 1: Seja o operador linear $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ tal que:

$$T(1, 2) = (-5, 12) \text{ e } T(-1, 1) = (-4, 3)$$

Determinar $T(x, y)$

Solução:

A transformação linear T pode ser escrita na forma matricial por

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Tal matriz transforma os vetores $(1, 2)$ e $(-1, 1)$ nos vetores $(-5, 12)$ e $(-4, 3)$, respectivamente.

Portanto, tem-se que:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} -5 \\ 12 \end{pmatrix}$$

$$\text{e } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -4 \\ 3 \end{pmatrix}$$

Isto é, o mesmo que resolver os sistemas lineares:

$$\begin{cases} a + 2b = -5 \\ -a + b = -4 \end{cases} \quad \text{e} \quad \begin{cases} c + 2d = 12 \\ -c + d = 3 \end{cases}$$

Ambos os sistemas podem ser resolvidos simultaneamente utilizando a notação matricial com operações elementares sobre linhas.

$$\left(\begin{array}{cc|c|c} 1 & 2 & -5 & 12 \\ -1 & 1 & -4 & 3 \end{array}\right) \longrightarrow L_2 \longrightarrow L_1 + L_2$$

$$\left(\begin{array}{cc|c|c} 1 & 2 & -5 & 12 \\ 0 & 3 & -9 & 15 \end{array}\right) \longrightarrow L_2 \longrightarrow \tfrac{1}{3} \cdot L_2$$

$$\left(\begin{array}{cc|c|c} 1 & 2 & -5 & 12 \\ 0 & 1 & -3 & 5 \end{array}\right) \longrightarrow L_1 \longrightarrow L_1 - 2 \cdot L_2$$

$$\left(\begin{array}{cc|c|c} 1 & 0 & 1 & 2 \\ 0 & 1 & -3 & 5 \end{array}\right)$$

Portanto, $a = 1, b = -3, c = 2$ e $d = 5$.

Exemplo 2: Encontrar $T(x, y)$ do exemplo 1, considerando $\mathbb{Z}_{26}$.

Solução:

Em $\mathbb{Z}_{26}$ tem-se que:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 21 \\ 12 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 25 \\ 1 \end{pmatrix} = \begin{pmatrix} 22 \\ 3 \end{pmatrix}$$

Os sistemas lineares correspondentes são:

$$\begin{cases} a + 2b = 21 \\ 25a + b = 22 \end{cases} \quad \text{e} \quad \begin{cases} c + 2d = 12 \\ 25c + d = 3 \end{cases}$$

Nesse caso, também serão realizados operações elementares sobre linhas, na notação matricial, mas considerando o módulo 26.

$$\left(\begin{array}{cc|c|c} 1 & 2 & 21 & 12 \\ 25 & 1 & 22 & 3 \end{array}\right) \longrightarrow L_2 \longrightarrow L_1 + L_2$$

$$\left(\begin{array}{cc|c|c} 1 & 2 & 21 & 12 \\ 26 & 3 & 43 & 15 \end{array}\right) \equiv \left(\begin{array}{cc|c|c} 1 & 2 & 21 & 12 \\ 0 & 3 & 17 & 15 \end{array}\right) \longrightarrow L_2 \longrightarrow 9 \cdot L_2$$

$$\left(\begin{array}{cc|c|c} 1 & 2 & 21 & 12 \\ 0 & 27 & 153 & 135 \end{array}\right) \equiv \left(\begin{array}{cc|c|c} 1 & 2 & 21 & 12 \\ 0 & 1 & 23 & 5 \end{array}\right) \longrightarrow L_1 - 2 \cdot L_2$$

$$\left(\begin{array}{cc|c|c} 1 & 0 & -25 & 2 \\ 0 & 1 & 23 & 5 \end{array}\right) \equiv \left(\begin{array}{cc|c|c} 1 & 0 & 1 & 2 \\ 0 & 1 & 23 & 5 \end{array}\right)$$

Portanto, em $\mathbb{Z}_{26}$, $a = 1, b = 23, c = 2$ e $d = 5$

A relação entre matrizes e transformações lineares dadas na observação anterior, especificamente nos ítens b) e c), é um caso particular da definição a seguir.

Definição 2: Sejam V e W espaços vetoriais de dimensão finita com bases α e β respectivamente, onde $\alpha = \{v_1, v_2, \ldots, v_n\}$. Se $T : V \longrightarrow W$ é uma transformação linear, então a matriz denotada por $[T]^{\alpha}_{\beta}$ e definida por

$$[T]^{\alpha}_{\beta} = \Big([T(v_1)]_{\beta} \quad [T(v_2)]_{\beta} \quad \ldots \quad [T(v_n)]_{\beta}\Big)$$

é chamada a matriz de T em relação às bases α e β.

(O vetor coluna $[T(v_i)]_{\beta}$) é o vetor de coordenadas de $T(v_i)$ em relação à base β).

Observe que se $V = \mathbb{R}^n$, $W = \mathbb{R}^m$ e α e β são as bases canônicas de $\mathbb{R}^n$ e $\mathbb{R}^m$ respectivamente, então $[T]^{\alpha}_{\beta} = [T]$ é a matriz canônica de T. A matriz $[T]^{\alpha}_{\beta}$ é tal que $[T]^{\alpha}_{\beta}[v]_{\alpha} = [T(v)]_{\beta} \ \ \forall\, v \in V$. Vide demonstração em Poole (2006, p.449).

Teorema 1: Seja V um espaço vetorial com bases α e β, e seja $T : V \longrightarrow V$ um operador linear. Então

$$[T]^{\beta}_{\beta} = P^{-1}[T]^{\alpha}_{\alpha}P$$

onde $P = [I]^{\beta}_{\alpha}$ é a matriz de mudança de coordenadas, da base β para α. Vide demonstração em Poole (2006, p. 458).

No que segue, a matriz A é considerada como a matriz canônica de um operador linear $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$.

Definição 3: Uma matriz quadrada A é dita *diagonalizável* se existir uma matriz invertível P tal que $P^{-1}AP$ é uma matriz diagonal; dizemos, então que a matriz P *diagonaliza* A.

Teorema 2: *Teorema Espectral para Matrizes Simétricas* Seja A uma matriz real $n \times n$. Então A será simétrica se, e somente se, for ortogonalmente diagonalizável. Ou seja, se existirem matrizes P ortogonal e D diagonal, tais que $P^tAP = D$.

Vide demonstração em Anton (2001, p. 251)

Definição 4: *Forma Quadrática no Espaço Tridimensional*

Uma forma quadrática em n variáveis é uma função $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ da forma

$$f(x) = X^TAX$$

onde A é uma matriz simétrica $n \times n$ e x é um vetor de $\mathbb{R}^n$, digamos $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$.

Exemplo 3: Determine a forma quadrática que tem como matriz associada a matriz $A = \begin{pmatrix} 1 & 3 \\ 3 & -7 \end{pmatrix}$.

Solução: Se $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, então

$$f(x) = X^T AX = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 3 & -7 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1^2 - 7x_2^2 + 6x_1x_2$$

Exemplo 4: Encontre a matriz associada à forma quadrática

$$f(x_1, x_2, x_3) = 5x_1^2 - 2x_2^2 + 3x_3^2 - 8x_1x_2 + 7x_2x_3$$

Solução:
$A = \begin{pmatrix} 5 & -4 & 0 \\ -4 & -2 & \frac{7}{2} \\ 0 & \frac{7}{2} & 3 \end{pmatrix}$ e portanto $f(x_1, x_2, x_3) = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 5 & -4 & 0 \\ -4 & -2 & \frac{7}{2} \\ 0 & \frac{7}{2} & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.

A seguir será descrito o processo chamado de diagonalização de formas quadráticas.

Seja $f(x) = X^T AX$ uma forma quadrática em n variáveis, na qual A é uma matriz simétrica $n \times n$. Pelo Teorema 2 desta seção, existe uma matriz ortogonal P que diagonaliza A. Isto é, $P^t AP = D$, onde D é diagonal. Considere $X = Py$ ou, equivalentemente, $y = P^{-1}X = P^t X$.

Substituindo na forma quadrática tem-se

$$X^t AX = (Py)^t A(Py) = y^t P^t APy = y^t Dy$$

que é uma forma quadrática sem termos mistos, pois D é diagonal. Se

$$D = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix} \text{ e } y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

então a forma quadrática nas novas variáveis passa a ser

$$y^t Dy = \lambda_1 y_1^2 + \ldots + \lambda_n y_n^2$$

neste caso, D é a matriz diagonal associada à forma quadrática diagonalizada.

3 CIFRAS DE HILL

Como dito anteriormente, a Cifra de Hill é um um sistema poligráfico de cifragem baseado em transformações matriciais. Ou seja, é uma cifra de substituição alfabética em bloco de tamanho fixo.

A chave de cifragem é uma matriz quadrada invertível módulo 26, enquanto a chave de decifragem é a sua matriz inversa.

Para cifrar uma determinada mensagem, é necessário que inicialmente seja estabelecida uma correspondência entre cada letra do alfabeto e um número inteiro. Excetuando-se o Z, as demais letras serão associadas ao valor numérico que indica a sua posição no alfabeto, conforme a tabela (2).

3.1 Processo de Cifragem

O processo de encriptação começa dividindo-se o texto em blocos de n letras. Como exemplo será utilizado $n = 2$, para melhor compreensão do leitor. O procedimento para cifragem é descrito detalhadamente a seguir.

- Agrupam-se as letras do texto duas a duas, fazendo a correspondência numérica conforme a tabela (2).
- Escolhe-se uma matriz A em $M_2(\mathbb{Z}_m)$ invertível. Essa matriz será a chave de cifragem.
- Cada par de letras será considerado um vetor coluna (p) formado pelos respectivos correspondentes numéricos. Este vetor é chamado de *vetor comum*.
- Efetua-se o produto $A \cdot p$. O resultado obtido é denominado de *vetor cifrado*.
- Finalmente, associam-se os valores obtidos em cada vetor cifrado às letras correspondentes e então tem-se o texto encriptado. Caso as entradas do vetor cifrado sejam

Tabela 2 - Correspondência Alfabético Numérica

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

números inteiros maiores que 26, aplicam-se os conceitos de aritmética modular para obter o correspondente alfabético conforme a tabela (2).

Exemplo 1: Cifragem da mensagem ÁLGEBRA.

- Divide-se a palavra em blocos de duas letras. Como a palavra possui quantidade ímpar de letras, acrescenta-se qualquer letra no último bloco para garantir a formação dos pares.

$$\text{ÁL} \quad \text{GE} \quad \text{BR} \quad \text{AZ}$$

- Associa-se à cada letra o correspondente numérico, escrevendo o par de números como o vetor coluna (p).

Á	L	G	E	B	R	A	Z
1	12	7	5	2	18	1	26

Assim, $p_1 = \begin{pmatrix} 1 \\ 12 \end{pmatrix}$, $p_2 = \begin{pmatrix} 7 \\ 5 \end{pmatrix}$, $p_3 = \begin{pmatrix} 2 \\ 18 \end{pmatrix}$ e $p_4 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

- A matriz [1] escolhida para a cifragem de cada vetor (p) é dada por:

$$A = \begin{pmatrix} 3 & 0 \\ 1 & 5 \end{pmatrix}$$

- Cifragem do par AL.

$$\begin{pmatrix} 3 & 0 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 12 \end{pmatrix} = \begin{pmatrix} 3 \\ 61 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 9 \end{pmatrix} \pmod{26}$$

Como 61 não possui correspondente alfabético, devemos substituí-lo pelo seu equivalente módulo 26, a saber, 9.

- Cifrando os demais pares:

$$\begin{pmatrix} 3 & 0 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 5 \end{pmatrix} = \begin{pmatrix} 21 \\ 32 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 6 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 3 & 0 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 18 \end{pmatrix} = \begin{pmatrix} 6 \\ 92 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 14 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 3 & 0 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

[1] A escolha dessa matriz é aleatória, desde que seja invertível módulo 26

- Novamente utilizando a tabela (2), obtemos a encriptação do texto.

CI UF FN CA

A transmissão dessa mensagem seria realizada como uma única cadeia, sem espaços:

CIUFFNCA

No exemplo, o texto foi dividido em blocos de 2 letras e cifrado por uma matriz de ordem 2. Esse processo é chamado **2-cifra de Hill**.

Assim, para blocos de n letras cifrados por matrizes de ordem n utiliza-se a cifragem **n-cifra de Hill**.

3.2 Processo de Decifragem

Para decifrar o texto "CIUFFNCA" realiza-se procedimento análogo ao de cifragem.

- Divide-se o texto cifrado em blocos de duas letras.
- Associa-se à cada letra o correspondente numérico conforme tabela (2), escrevendo o par de números como o vetor coluna (c). É fácil perceber que $c = A \cdot p$, já que o objetivo do processo de decifragem é a obtenção do vetor p. Assim, multiplicando-se a igualdade anterior por A^{-1} pela esquerda, o vetor p é facilmente encontrado.
- Efetua-se o produto $A^{-1} \cdot c$.
- Ao resultado obtido repete-se, novamente, a correspondência alfabética, aplicando a congruência módulo 26, se necessário, e a decifragem é concluída.

Exemplo 2: Decifrando o texto CIUFFNCA.

- Os equivalentes numéricos, agrupados dois a dois, do texto são:

$$3 \quad 9 \qquad 21 \quad 6 \qquad 6 \quad 14 \qquad 3 \quad 1$$

- A inversa da matriz A é dada por:

$$A^{-1} = \begin{pmatrix} 9 & 0 \\ 19 & 21 \end{pmatrix}$$

- Decifragem dos vetores cifrados:

$$\begin{pmatrix} 9 & 0 \\ 19 & 21 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 9 \end{pmatrix} = \begin{pmatrix} 27 \\ 246 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 12 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 9 & 0 \\ 19 & 21 \end{pmatrix} \cdot \begin{pmatrix} 21 \\ 6 \end{pmatrix} = \begin{pmatrix} 189 \\ 525 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 5 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 9 & 0 \\ 19 & 21 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 54 \\ 408 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 18 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 9 & 0 \\ 19 & 21 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 27 \\ 78 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{26}$$

- Cada vetor coluna decifrado corresponde exatamente ao texto original ÁLGEBRAZ.

3.3 **Abordagem Alternativa**

Uma forma interessante de aplicar o método é apresentar a matriz codificadora como a matriz diagonal D da nova forma quadrática diagonalizada y^tDy, obtida após utilizar o processo de diagonalização em uma forma quadrática X^tAX, conforme descrito na seção 2.4. Obviamente que a matriz A da forma quadrática inicial deve ser escolhida invertível em $\mathbb{Z}_{26}$ de modo que D seja invertível. Para isso, é necessário que as raízes do polinômio caracterísco de A sejam números inteiros tais que quando reduzidos módulo 26, sejam invertíveis em $\mathbb{Z}_{26}$. Nesse caso, a matriz diagonal D será invertível módulo 26, pois U_{26} é fechado para a multiplicação. De outro modo, a matriz simétrica A deve ser tal que seus autovalores sejam números inteiros invertíveis em $\mathbb{Z}_{26}$.

Exemplo 1: Cifrando o texto MEU REINO POR UM CAVALO como uma **3-cifra de Hill**.

Considere a forma quadrática [2]

$$X^TAX = -x^2 + 5y^2 + 5z^2 - 4yz$$

[2] A forma quadrática indicada foi escolhida aleatoriamente mantendo-se os critérios já apresentados sobre a matriz codificadora.

Tal forma pode ser representada, matricialmente, por

$$X^T AX = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 5 & -2 \\ 0 & -2 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

tem-se que $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 5 & -2 \\ 0 & -2 & 5 \end{pmatrix}$ é a matriz simétrica dessa forma quadrática.

Como $detA = -21 \equiv 5 \pmod{26}$, A e D são invertíveis.

Para achar D, devemos encontrar os autovalores de A, resolvendo a equação característica a seguir.

$$det(A - \lambda I) = \begin{vmatrix} -1-\lambda & 0 & 0 \\ 0 & 5-\lambda & -2 \\ 0 & -2 & 5-\lambda \end{vmatrix} = 0$$

Desenvolvendo o determinante obtem-se o polinômio $-\lambda^3 + 9\lambda^2 - 11\lambda - 21 = 0$, cujas raízes são $\lambda_1 = -1$, $\lambda_2 = 3$ e $\lambda_3 = 7$.

Assim,

$$D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix}$$

- Agrupando-se as letras do texto em blocos de três e fazendo a correspondência numérica conforme tabela (2) tem-se que:

M	E	U		R	E	I		N	O	P		O	R	U		M	C	A
13	5	21		18	5	9		14	15	16		15	18	21		13	3	1

V	A	L		O	X	X
22	1	12		15	24	24

- Os cálculos para cifrar os sete vetores correspondentes são:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 5 \\ 21 \end{pmatrix} = \begin{pmatrix} -13 \\ 15 \\ 147 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 15 \\ 17 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 18 \\ 5 \\ 9 \end{pmatrix} = \begin{pmatrix} -18 \\ 15 \\ 63 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 15 \\ 11 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 15 \\ 16 \end{pmatrix} = \begin{pmatrix} -14 \\ 45 \\ 112 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 19 \\ 8 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 18 \\ 21 \end{pmatrix} = \begin{pmatrix} -15 \\ 54 \\ 147 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 2 \\ 17 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -13 \\ 9 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 9 \\ 7 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 22 \\ 1 \\ 12 \end{pmatrix} = \begin{pmatrix} -22 \\ 3 \\ 84 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 3 \\ 6 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 24 \\ 24 \end{pmatrix} = \begin{pmatrix} -15 \\ 72 \\ 168 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 20 \\ 12 \end{pmatrix} \pmod{26}$$

Portanto, a mensagem será transmitida por MOQHOKLSHKBQMIGDCFKTL.

A cifragem foi realizada com a matriz diagonal, pois a obtenção de sua inversa pode ser facilmente calculada, tornando este exemplo mais didático.

Observação: Outra escolha interessante é considerar uma matriz codificadora A involutória. Isto é, A tal que $A^2 = I$. Neste caso tem-se que $A^{-1} = A$ e portanto a mesma matriz que codifica, também decodifica as mensagens. Este fato pode motivar alunos e professores, visto que as propriedades algébricas de alguns elementos tem um potencial prático.

O processo de decifragem do texto segue exatamente o procedimento indicado na 2-cifra de Hill exibido no início deste capítulo.

3.4 **Fragilidade do Método**

A natureza linear da Cifra de Hill, imposta pelas operações utilizadas nos processos de cifragem e decifragem, a torna vulnerável à ataques e consequentes violações de sigilo das informações cifradas, através desse método.

Se o texto transmitido for interceptado e o interceptador conhecer alguns pares de caracteres originais e cifrados, ele descobrirá a chave codificadora/decodificadora. Isto,

pois sabe-se que a matriz codificadora, vista como uma matriz sobre $\mathbb{R}$, está associada à uma transformação linear, e toda transformação linear $T : V \longrightarrow W$ pode ser determinada apenas a partir dos valores em uma base de V, conforme descrito na seção 2.4.

Para ilustrar tal fragilidade será utilizado como exemplo uma 2-cifra de Hill. A partir do conhecimento de apenas quatro caracteres originais e sua respectiva cifragem, será obtida a matriz decodificadora e, consequentemente a matriz codificadora.

Sabendo-se que a mensagem YUQHTMLCFGUMNMMT inicia-se originalmente com as sílabas AOIN, portanto fazendo a correspondência numérica conforme a tabela (2), tem-se que

A	O		I	N
1	15		9	14

e o correspondente numérico do texto cifrado é:

Y	U		Q	H
25	21		17	8

A questão agora é descobrir a matriz que transforma os vetores

$$c_1 = \begin{pmatrix} 25 \\ 21 \end{pmatrix} \text{ e } c_2 = \begin{pmatrix} 17 \\ 8 \end{pmatrix}$$

nos vetores

$$p_1 = \begin{pmatrix} 1 \\ 15 \end{pmatrix} \text{ e } p_2 = \begin{pmatrix} 9 \\ 14 \end{pmatrix}$$

Seja $A^{-1} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ essa matriz.
Pelo procedimento de decifragem, tem-se que

$$A^{-1} \cdot c_1 = p_1 \quad \text{e} \quad A^{-1} \cdot c_2 = p_2.$$

As sentenças acima podem ser escritas como

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} 25 \\ 21 \end{pmatrix} = \begin{pmatrix} 1 \\ 15 \end{pmatrix}$$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 8 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \end{pmatrix}$$

Ou seja, o equivalente a resolver, em $\mathbb{Z}_{26}$, os sistemas lineares a seguir

$$\begin{cases} 25x + 21y = 1 \\ 17x + 8y = 9 \end{cases} \text{ e } \begin{cases} 25z + 21w = 15 \\ 17z + 8w = 14 \end{cases}$$

Como ambos sistemas tem a mesma matriz dos coeficientes, é possível resolvê-los simultaneamente através de operações elementares sobre linhas e a aritmética modular.

$$\left(\begin{array}{cc|c|c} 25 & 21 & 1 & 15 \\ 17 & 8 & 9 & 14 \end{array}\right) \rightarrow \text{Sistemas escritos na forma matricial.}$$

$$\left(\begin{array}{cc|c|c} 625 & 525 & 25 & 375 \\ 17 & 8 & 9 & 14 \end{array}\right) \equiv \left(\begin{array}{cc|c|c} 1 & 5 & 25 & 11 \\ 17 & 8 & 9 & 14 \end{array}\right) \rightarrow 25 \cdot L_1.$$

$$\left(\begin{array}{cc|c|c} 1 & 5 & 25 & 11 \\ 0 & -77 & -416 & -173 \end{array}\right) \equiv \left(\begin{array}{cc|c|c} 1 & 5 & 25 & 11 \\ 0 & 1 & 0 & 9 \end{array}\right) \rightarrow L_2 - 17 \cdot L_1.$$

$$\left(\begin{array}{cc|c|c} 1 & 0 & 25 & -34 \\ 0 & 1 & 0 & 9 \end{array}\right) \equiv \left(\begin{array}{cc|c|c} 1 & 0 & 25 & 18 \\ 0 & 1 & 0 & 9 \end{array}\right) \rightarrow L_1 - 5 \cdot L_2.$$

Portanto, $x = 25, y = 0, z = 18$ e $w = 9$ e $A^{-1} = \begin{pmatrix} 25 & 0 \\ 18 & 9 \end{pmatrix}$.

Aplicando-se a matriz decodificadora A^{-1} aos demais pares de caracteres, obtém-se a mensagem original, a saber: AO INFINITO E ALÉM X. Os cálculos foram omitidos, pois são análogos aos já realizados neste capítulo.

4 CRIPTOGRAFIA NO ENSINO MÉDIO

No início desta dissertação afirmou-se que é possível e necessário que o professor de Matemática da Educação Básica busque situações que favoreçam uma prática docente e discente voltada para o desenvolvimento de características próprias da Matemática.

Muitas vezes, isso implica em sair do senso comum que orienta a prática tradicional de ensino da disciplina. Implica na criação ou adaptação de práticas que sejam realmente desafiadoras para os alunos, que lhes façam sentido. A ideia deve ultrapassar o íntimo desejo de muitos professores em despertar a paixão pela Matemática. As aulas precisam ser planejadas para atrair também a atenção e o envolvimento daqueles que sequer pensavam que tinham aptidão para lidar com assuntos de natureza matemática, em função das experiências anteriores que tiveram em sua vida escolar e que não proporcionaram tal descoberta. Uma pessoa que aprecie Matemática não precisa necessariamente desejar seguir uma carreira que tenha por base o conhecimento aprofundado de alguns de seus princípios.

Entretanto, sabemos que apenas a vontade do professor de Matemática nem sempre é suficiente para concretizar de forma satisfatória uma prática docente diferenciada, que atraia o aluno para o verdadeiro significado da construção do conhecimento matemático.

Diante dessa realidade, é fundamental que as instituições de Ensino Médio comecem a promover iniciativas pedagógicas que permitam, incentivem e proporcionem o desenvolvimento de práticas de iniciação à pesquisa científica nas diversas áreas do conhecimento.

Foi exatamente a oportunidade de estar atuando em uma instituição de Ensino Médio que promoveu esse tipo de iniciativa pedagógica - dentre outras de igual importância para a formação integral do indivíduo - que motivou o desenvolvimento do tema dessa dissertação.

Desde o ano letivo de 2010, faço parte do quadro de educadores da Escola Sesc de Ensino Médio - ESEM, uma escola que nasceu, e cresce a cada ano, a partir de uma proposta diferenciada de educação e promoção humana. Dentre as diversas iniciativas lá desenvolvidas que pretendem atender a esse propósito, está o PIC - Programa de Iniciação Científica. Nele, todos os educadores que atuam ministrando aulas regulares das disciplinas das áreas de Ciências da Natureza, Ciências Humanas, Códigos e Linguagens e Matemática tem também a oportunidade ímpar de atuarem como orientadores de trabalhos de iniciação científica juntos aos jovens matriculados nas três séries do Ensino Médio. Apesar de ser facultativa aos alunos da terceira série, a maioria deles adere a algum dos temas propostos pelos professores orientadores. Uma característica peculiar do PIC realizado na ESEM é possibilitar a integração dos alunos das três séries do Ensino Médio num mesmo grupo de iniciação científica, uma vez que a escolha do tema de pesquisa é feita

pelos próprios alunos, a partir dos temas ofertados pelos professores orientadores. Ou seja, não existe a barreira que uma suposta seriação poderia acarretar. Afinal, através do PIC, é possível reafirmar que a construção do conhecimento se dá pela integração de diversos saberes e que o alcance destes não depende necessariamente do formato de distribuição de conteúdos do currículo escolar.

Em 2013, iniciei a procura pelo tema que nortearia as atividades de investigação científica sob minha orientação naquele ano letivo. A ideia era propor um tema atual, que estivesse presente no dia a dia dos estudantes, provocando um desejo natural pelo aprendizado dos aspectos que envolveriam esse tema. Em particular, a compreensão de como a Matemática pode se fazer presente enquanto ferramenta fundamental para o seu desenvolvimento.

A Criptografia apareceu como tema viável exatamente por estar vinculada ao maior, senão mais querido, veículo de comunicação da atualidade: a Internet. Sem as técnicas criptográficas que zelam pela integridade e proteção das informações transmitidas e armazenadas, a maioria dos processos realizados, via internet, não seriam possíveis.

Definido o tema de pesquisa do PIC-ESEM/2013, muitos alunos desejaram participar dessa proposta, mas havia apenas quatro vagas e dessa forma quatro alunos foram sorteados para integrarem aquele grupo de pesquisa. Importante mencionar que até a apresentação da proposta de trabalho, nenhum deles tinha qualquer conhecimento prévio sobre o significado e a aplicação da Criptografia.

As atividades de orientação foram desenvolvidas durante cerca de seis meses, em encontros semanais com duração de quarenta e cinco minutos. A cada encontro uma tarefa era proposta, discutida, apresentada, avaliada ou redefinida, de acordo com os avanços obtidos pelos alunos.

Inicialmente, os alunos foram apresentados ao tema Criptografia e incentivados a realizarem as primeiras pesquisas sobre ele para que começassem a se familiarizar com suas características e também com próprio método científico.

Em pouco tempo perceberam que se tratava de um tema extenso e que os conceitos matemáticos envolvidos nos modernos processos criptográficos eram muito complexos para o nível escolar no qual se encontravam. Esse fato serviu para lhes mostrar como um trabalho de pesquisa é árduo e que, na maioria das vezes, os seus rumos precisam ser corrigidos.

No caso citado, a correção de rumo foi proposta através do estudo do processo criptográfico já descrito no capítulo 3 - a Cifra de Hill. A escolha desse processo permitiu que os alunos pesquisassem conteúdos matemáticos - Matrizes e noções de Aritmética Modular - com grau de dificuldade mais apropriado ao nível de escolaridade e formação que dispunham, embora não pertencessem à série do Ensino Médio que cursavam.

Com base no material até então pesquisado e discutido dentro e fora dos encontros semanais de orientação, o grupo partiu para a elaboração de um roteiro de pesquisa e

produção do trabalho, conforme segue:

1. **Criptografia**:
    - O que é?
    - Para que serve?
    - Onde é aplicada?
    - Aspectos históricos.
    - Imagens/exemplos.
2. **Matrizes**:
    - Definição
    - Tipo de Matrizes
    - Matriz Identidade
    - Operações (multiplicação) / comutatividade
    - Matriz Inversa
3. **Aritmética Modular**:
    - Definição
    - Propriedades elementares
    - Congruência módulo 26
4. **Cifra de Hill**:
    - Descrição do método
    - Aplicação
    - Exemplos resolvidos
5. **Conclusão**:
    - Aplicação do estudo de Matrizes e Aritmética Modular em Criptografia.
    - Importância da criptografia nas trocas de informação, via internet.

Naturalmente, esse roteiro sofreu algumas alterações ao longo do processo de elaboração do trabalho. Porém, demonstra como os alunos conseguiram, em pouco mais de um mês de atividades semanais, compreender como estruturar um trabalho que envolva pesquisa científica.

Decidido qual método criptográfico seria abordado durante a pesquisa, o grupo foi dividido em duplas e o estudo sobre Matrizes foi iniciado. Durante os encontros as duplas recebiam as mesmas tarefas semanais, iniciavam os primeiros estudos sob minha orientação e supervisão, apresentavam pequenos semninários e discutiam os resultados encontrados. No fim de cerca de dois meses, o grupo construiu os conceitos de Matrizes necessários ao prosseguimento do trabalho.

O próximo passo foi apresentar noções elementares de Aritmética Modular que permitissem a compreensão de sua funcionalidade no método de cifragem de Hill. Por se tratar de um conteúdo mais complexo e inerente aos cursos de graduação em Matemática, somente a definição e as propriedades mais simples foram exploradas com os alunos, através de alguns exemplos apresentados nos encontros. Essa abordagem foi realizada por cerca de um mês.

Após o término do estudo dos conteúdos matemáticos citados, o grupo estava apto para compreender o processo de criptografia utilizando a Cifra de Hill. No início, os alunos cifraram e decifraram palavras. Com maior domínio sobre a técnica, passaram a cifrar e decifrar mensagens que trocavam uns com os outros, como em uma brincadeira.

Importante ressaltar que as pesquisas sobre os aspectos que permeiam o desenvolvimento da criptografia e sua importância na atualidade foram realizadas pelo grupo nas primeiras semanas de pesquisa, quando ainda não havia sido feita a opção pelo estudo da Cifra de Hill como exemplo de técnica criptográfica.

Os resultados da pesquisa foram apresentados em novembro de 2013, durante a Escola Aberta, evento promovido anualmente pela ESEM no qual diversos trabalhos de diferentes áreas são divulgados para a comunidade escolar e visitantes, entre eles os resultados das pesquisas desenvolvidas durante o PIC.

A apresentação do trabalho durou cerca de vinte minutos. O formato assemelha-se muito ao utilizado em comunicações científicas apresentadas em congressos. Os alunos se revezaram e fizeram uma síntese da proposta de pesquisa, dos conceitos matemáticos estudados, da metodologia que envolve a Cifra de Hill e apresentaram os resultados obtidos. Merece destaque o momento em que um dos alunos encaminhou-se até o quadro branco, cifrou e decifrou a palavra "gato", detalhando para os ouvintes todo o processo matemático envolvido.

Ao final, professores e alunos presentes à apresentação (a presença de alunos é livre e acontece de acordo com interesse que os temas despertam nos mesmos!) fizeram perguntas e interagiram com o grupo, tirando as eventuais dúvidas que surgiram.

A experiência narrada neste capítulo reafirma o quanto é possível realizar uma

prática de ensino de Matemática contextualizada e integrada com a realidade. Mostra como é possível despertar nos alunos, o interesse em aprender conceitos matemáticos acima de sua escolaridade. Mostra a funcionalidade da Matemática e pode minimizar a falsa ideia de que Matemática só pode ser aprendida e admirada por um grupo seleto. É preciso mudar essa ideia. É preciso dar oportunidade para que os alunos experimentem a Matemática de verdade e que, a partir dessa vivência, façam sua escolha por seguir (ou não) caminhos que necessitem de seus conhecimentos.

Para aqueles que eventualmente argumentem que nem todas as escolas oferecem a oportunidade de trabalho ilustrada e, por isso, é impossível realizá-la em grande escala, segue minha total concordância, conforme mencionado no início do capítulo. Porém, segue também o meu desejo em divulgar essa experiência para, quem sabe num futuro próximo, essa realidade possa ser transformada, a partir de iniciativas similares.

CONCLUSÃO

O processo de orientação e supervisão do trabalho de iniciação científica vivenciados junto ao grupo de alunos da segunda série do Ensino Médio foi a ferramenta essencial para a elaboração da proposta desta dissertação. Ele permitiu a análise, a correção e a sugestão de alguns aspectos que contribuirão para que a realização de futuros trabalhos baseados no tema sejam mais bem elaborados e contribuam tanto para os professores quanto para os alunos aprenderem mais sobre Criptografia e sua abordagem nas aulas de Matemática.

Em primeiro lugar, ficou clara a importância de um maior aprofundamento em relação aos aspectos históricos que envolvem o desenvolvimento da Criptografia. O resultado dessa percepção culminou na produção do capítulo 1 deste trabalho.

Outro aspecto que mereceu atenção foi a apresentação detalhada, no capítulo 2, dos conceitos elementares sobre Álgebra Linear e Aritmética Modular utilizados no processo criptográfico exemplificado. O leitor deve ter percebido que esses conceitos foram abordados em um nível superior ao que deve ser apresentado em aulas do Ensino Médio. Neste caso, o objetivo foi prover o professor de elementos de revisão de conteúdos que foram vistos em sua formação acadêmica. Caberá a cada docente adaptar a linguagem de apresentação desses conteúdos, de acordo com as características de suas turmas.

Em relação à descrição da Cifra de Hill, além dos detalhes matemáticos essenciais à boa compreensão dos processos de encriptação e decriptação, os aspectos que causam a fragilidade desse processo como ferramenta segura de transmissão de informações também foram acrescentados e exemplificados.

Por fim, espera-se que este trabalho possa realmente despertar em professores e alunos uma vontade diferente de ensinar e aprender Matemática utilizando a Criptografia como motivação. Ou se preferirem, aprender um pouco de Criptografia, a partir da Matemática.

O mais importante é que compreendam que é possível viabilizar o ensino e aprendizagem de forma diferenciada, por meio da pesquisa, da análise, da discussão, da modelagem, partindo da compreensão histórica e social de temas relevantes para a sociedade e que, de alguma forma, a Matemática se faz presente neles.

REFERÊNCIAS

ANTON, H.; RORRES, C. *Álgebra Linear com aplicações*. 8. ed. Porto Alegre: Bookman, 2001.

BOLDRINI, J. L. et al. *Álgebra Linear*. 3. ed. São Paulo: HARBRA ltda, 1980.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2. ed. Rio de Janeiro: IMPA, 2009.

COUTO, S. P. *Códigos cifras*. 1. ed. Rio de Janeiro: Novaterra, 2008.

DUMMIT, D. S.; FOOTE, R. M. *Abstract Algebra*. 2. ed. USA: Wiley, 1999.

HEFEZ, A. *Elementos de Aritmética*. 2. ed. Rio de Janeiro: SBM, 2011.

IEZZI, G.; HAZZAN, S. *Fundamentos da matemática elementar 4*. 7. ed. São Paulo: Atual, 2004.

SHOKRANIAN, S. *Criptografia para iniciantes*. 1. ed. Brasília: UnB, 2005.

SINGH, S. *O livro dos códigos*. 5. ed. Rio de Janeiro: Record, 2005.

STEINBRUCH, A.; WINTERLE, P. *Álgebra Linear*. 2. ed. São Paulo: Pearson Makron Books, 1987.